(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 22 220 A 1**

(51) Int. Cl.[6]: G 06 K 19/073

(21) Aktenzeichen: 198 22 220.3
(22) Anmeldetag: 18. 5. 98
(43) Offenlegungstag: 25. 11. 99

DE 198 22 220 A 1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Vater, Harald, Dr., 35398 Gießen, DE; Drexler, Hermann, Dr., 81371 München, DE; Johnson, Eric, 81371 München, DE

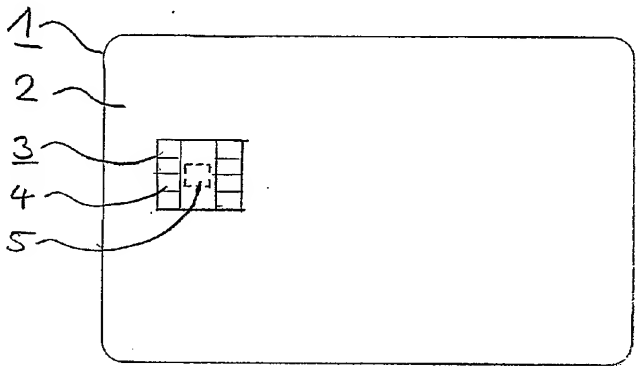
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 195 08 724 C1
DE 694 04 674 T2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Zugriffsgeschützter Datenträger

(57) Die Erfindung betrifft einen Datenträger (1), der einen Halbleiterchip (5) aufweist. Um zu verhindern, daß ein Angreifer aus abgehörten Signalverläufen des Chips (5) geheime Daten des Chips (5) ermittelt, werden sicherheitsrelevante Operationen nur mit bestimmten Befehlen des Betriebsprogramms durchgeführt, bei deren Verwendung aus den Signalverläufen nicht auf die verarbeiteten Daten geschlossen werden kann. Diese Befehle zeichnen sich dadurch aus, daß sie die Daten wenigstens byteweise verarbeiten, daß sie alle den gleichen oder einen ähnlichen Signalverlauf hervorrufen und/oder daß der von ihnen hervorgerufene Signalverlauf wenig oder gar nicht von den jeweils verarbeiteten Daten abhängt.



DE 198 22 220 A 1

Beschreibung

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z. B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombination des Anspruchs 1 gelöst.

Bei der erfindungsgemäßen Lösung werden im Gegensatz zum Stand der Technik keine Maßnahmen getroffen, um ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden statt dessen Maßnahmen getroffen, die es einem potentiellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Die Signalverläufe hängen von den Operationen ab, die der Chip gerade ausführt. Die Steuerung dieser Operationen erfolgt mit Hilfe eines Betriebsprogramms, das in einem Speicher des Chips gespeichert ist. Das Betriebsprogramm setzt sich aus einer Reihe von einzelnen Befehlen zusammen, die jeweils eine genau festgelegte Operation auslösen. Damit der Chip die ihm zugedachten Funktionen ausüben kann, ist für jede dieser Funktionen eine entsprechende Befehlsfolge zu definieren. Bei einer solchen Funktion kann es sich beispielsweise um das Verschlüsseln von Daten mit Hilfe eines geheimen Schlüssels handeln. Um einem Angreifer, der die Vorgänge auf dem Chip mittels von ihm dort angebrachten Mikrosonden abhört, möglichst wenig Informationen über die jeweils abgearbeiteten Befehle und die bei der Abarbeitung der Befehle verwendeten Daten zu geben, werden zur Realisierung einer gewünschten Funktion bevorzugt solche Befehle verwendet, bei denen ein Ausspähen von Informationen nur schwer oder gar nicht möglich ist. Mit anderen Worten, es sollen keine Befehle verwendet werden, bei denen durch Abhören auf einfache Art und Weise auf die verarbeiteten Daten geschlossen werden kann. Ein Rückschluß auf die Daten ist aber immer dann besonders einfach, wenn der Befehl nur sehr wenige Daten verarbeitet, beispielsweise nur ein einzelnes Bit. Aus diesem Grund werden gemäß der Erfindung zumindest für alle sicherheitsrelevanten Operationen, wie beispielsweise das Verschlüsseln von Daten, bevorzugt solche Befehle verwendet, die gleichzeitig mehrere Bits, z. B. jeweils ein Byte verarbeiten. Durch dieses gleichzeitige Verarbeiten mehrerer Bits verwischt der Einfluß, den die einzelnen Bits auf den durch den Befehl hervorgerufenen Signalverlauf haben zu einem Gesamtsignal, aus dem nur sehr schwer auf die einzelnen Bits zurückgeschlossen werden kann. Der Signalverlauf ist wesentlich komplexer als bei der Verarbeitung von einzelnen Bits und es ist nicht ohne weiteres ersichtlich, welcher Teil des Signals zu welchem Bit der verarbeiteten Daten gehört.

Zusätzlich oder alternativ hierzu kann gemäß der Erfindung der Angriff auf die verarbeiteten Daten dadurch erschwert werden, daß bei sicherheitsrelevanten Operationen ausschließlich solche Befehle verwendet werden, die einen identischen oder sehr ähnlichen Signalverlauf auslösen bzw. Befehle, bei denen die verarbeiteten Daten keinen oder nur einen sehr geringen Einfluß auf den Signalverlauf haben.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht und

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in **Fig.** 1 dargestellten Chipkarte in Aufsicht.

In **Fig.** 1 ist als ein Beispiel für den Datenträger eine Chipkarte **1** dargestellt. Die Chipkarte **1** setzt sich aus einem Kartenkörper **2** und einem Chipmodul **3** zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers **2** eingelassen ist. Wesentliche Bestandteile des Chipmoduls **3** sind Kontaktflächen **4**, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip **5**, der mit den Kontaktflächen **4** elektrisch verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen **4** kann auch eine in **Fig.** 1 nicht dargestellte Spule oder ein anderes Übertragungsmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip **5** und einem externen Gerät vorhanden sein.

In **Fig.** 2 ist ein stark vergrößerter Ausschnitt des Chips **5** aus **Fig.** 1 in Aufsicht dargestellt. Das besondere der **Fig.** 2 liegt darin, daß die aktive Oberfläche des Chips **5** dargestellt ist, d. h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips **5** schützen, sind in **Fig.** 2 nicht dargestellt. Um Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen **6** mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen **6**, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips **5** ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen **6** des Chips **5** mit Mikroson-

den zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips **5** erlangt.

Gemäß der Erfindung werden die Befehle des Betriebsprogramms des Chips wenigstens bei allen sicherheitsrelevanten Operationen so ausgewählt, daß aus den abgehörten Signalverläufen entweder überhaupt nicht oder zumindest nur sehr schwer Rückschlüsse auf die mit den Befehlen verarbeiteten Daten gezogen werden können. Dies kann beispielsweise dadurch erreicht werden, daß man bei Sicherheitsoperationen grundsätzlich auf alle Befehle verzichtet, die einzelne Bits verarbeiten, wie z. B. das Verschieben einzelner Bits, durch das eine Permutation der Bits einer Bitfolge bewirkt werden soll. Statt der Bitbefehle kann man beispielsweise auf Byte-Befehle zurückgreifen, wie beispielsweise Kopier- oder Rotationsbefehle, die statt eines einzelnen Bits gleich ein gesamtes Byte bestehend aus acht Bits verarbeiten. Der Byte-Befehl löst im Gegensatz zu dem Bit-Befehl einen wesentlich komplexeren Signalverlauf aus, wobei eine Zuordnung zwischen einzelnen Bits und Teilbereichen des Signalverlaufs extrem schwierig ist. Dies führt zu einer Verschleierung der mit dem Byte-Befehl verarbeiteten Information und erschwert somit ein Ausspähen dieser Information.

Weiterhin besteht im Rahmen der Erfindung noch die Möglichkeit, bei sicherheitsrelevanten Operationen grundsätzlich nur Befehle zu verwenden, die einen sehr ähnlichen Signalverlauf auslösen, so daß eine Unterscheidung der gerade abgearbeiteten Befehle anhand der Signalverläufe sehr schwierig ist. Ebenso ist es auch möglich, die Befehle so zu gestalten, daß die Art der verarbeiteten Daten keinen oder nur einen sehr geringen Einfluß auf den durch den Befehl ausgelösten Signalverlauf haben.

Die geschilderten Varianten können bezogen auf die einzelnen Befehle entweder alternativ oder in Kombination eingesetzt werden. Ein erfindungsgemäßer Satz von sicherheitsrelevanten Befehlen kann sich somit aus Befehlen zusammensetzen, die einer oder mehrerer der oben genannten Varianten angehören. Ebenso kann auch ein Befehlssatz verwendet werden, bei dem alle Befehle derselben Variante angehören,wobei auch zugelassen sein kann, daß einige oder auch alle Befehle darüber hinaus auch anderen Varianten angehören. So können beispielsweise ausschließlich Byte-Befehle zugelassen sein, wobei bevorzugt solche Befehle verwendet werden, die zudem einen sehr ähnlichen Signalverlauf auslösen.

Als sicherheitsrelevante Operationen sind z. B. Verschlüsselungsoperationen anzusehen, die häufig auch bei Chipkarten eingesetzt werden. Im Rahmen solcher Verschlüsselungen werden eine Reihe von Einzeloperationen ausgeführt, die zu bitweisen Veränderungen in einem Datenwort führen. Gemäß der Erfindung werden alle diese Befehle durch Byte-Befehle ersetzt und/oder es werden die weiteren oben genannten erfindungsgemäßen Maßnahmen getroffen. Auf diese Art und Weise wird es einem Angreifer noch weiter erschwert, aus den abgehörten Signalverläufen Rückschlüsse auf die bei der Verschlüsselung verwendeten geheimen Schlüssel zu ziehen und es wird dadurch ein Mißbrauch dieser geheimen Schlüssel verhindert.

Patentansprüche

1. Datenträger mit einem Halbleiterchip (**5**) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips (**5**) detektierbare Signale hervorruft, **dadurch gekennzeichnet**, daß der Datenträger bei der Durchführung sicherheitsrelevanter Operationen ausschließlich solche Befehle des Betriebsprogramms verwendet, bei denen aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann.

2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß die verwendeten Befehle, für eine wenigstens byteweise Verarbeitung von Daten ausgelegt sind.

3. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die verwendeten Befehle sich bezüglich der von ihnen hervorgerufenen Signalverläufe nicht oder nur sehr wenig voneinander unterscheiden.

4. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die verwendeten Befehle jeweils zu einem Signalverlauf führen, der nicht oder in einem nur sehr geringen Ausmaß von den mit dem Befehl verarbeiten Daten abhängt.

5. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei den sicherheitsrelevanten Operationen um Schlüsselpermutationen oder Permutationen anderer geheimer Daten handelt.

6. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei dem Datenträger um eine Chipkarte handelt.

Hierzu 1 Seite(n) Zeichnungen

Nummer: **DE 198 22 220 A1**
Int. Cl.[6]: **G 06 K 19/073**
Offenlegungstag: 25. November 1999

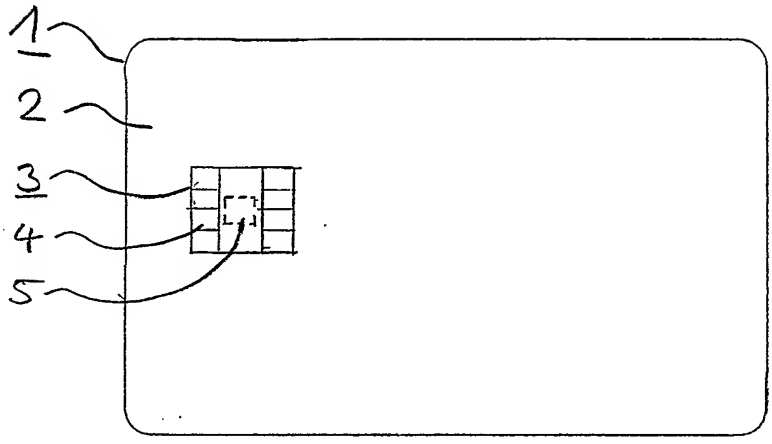


Fig. 1

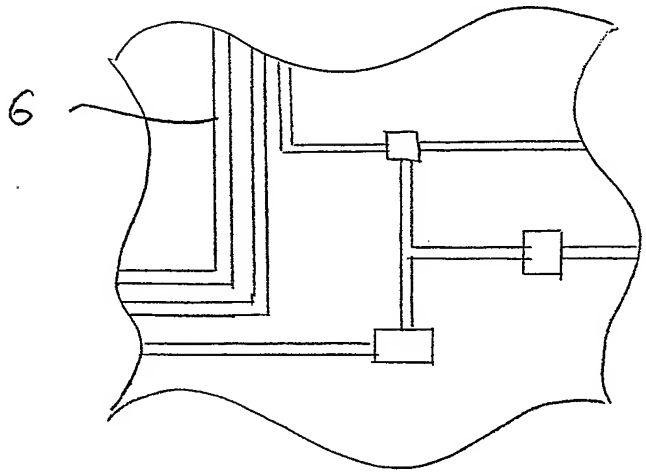


Fig. 2